UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/691,277	10/22/2003	Yoram Ofek	TFI 1848	4929

20787 7590 06/07/2007

SITRICK & SITRICK
8340 N LINCOLN AVENUE SUITE 201
SKOKIE, IL 60077

EXAMINER	
MORAN, RANDAL D	
ART UNIT	**PAPER NUMBER**
2135	

MAIL DATE	DELIVERY MODE
06/07/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/691,277	OFEK ET AL.	
	Examiner	Art Unit	
	Randal D. Moran	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 October 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-102* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-102* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/21/2003*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-102 are pending in the application.

2. Below, Examiner has pointed out particular references contained in the prior art(s) of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claims, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully each reference in its entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Information Disclosure Statement

1. The information disclosure statement filed 11/21/2003 fails to comply with 37 CFR 1.97, 1.98 and MPEP § 609 because it does not include a concise explanation of the relevance, as it is presently understood by the individual designated in 37 CFR 1.56(c) most knowledgeable about the content of the information. It has been placed in the application file, but the information referred to therein has not been considered as to the merits. Applicant is advised that the date of any re-submission of any item of

information contained in this information disclosure statement or the submission of any missing element(s) will be the date of submission for purposes of determining compliance with the requirements based on the time of filing the statement, including all certification requirements for statements under 37 CFR 1.97(e). See MPEP § 609.05(a).

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. **Claims 1-102** are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter, strictly software, as they do not fall under any of the statutory classes of inventions. The language in the claims raise an issue because the claims are directed merely to an abstract idea that is not tied to an article of manufacture which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. 101.

The claims could reasonably be drawn to functional descriptive material, per se, i.e., "program" may be taken to mean software alone, and as such, the claims would be directed to non-statutory subject matter. The claims read on software subject matter such as functions relating to software logic modules and logic programs (p. 3- lines 1-5, p. 9- lines 13-25).

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. **Claims 1, 31, 37, 52, 54-56, and 96** are rejected under 35 U.S.C. 102(e) as being anticipated by **Agrawal et al. (US 2002/0124169)**, hereafter "Agrawal".

3. Considering **Claims 1, 31, 37, 52, 54-56, and 96,** Agrawal discloses a communication method for authentication of communications of data packets ([0033] lines 1-3), the method comprising: defining rules of processing ([0038] lines 11-17); generating security tag vectors responsive to the rules of processing and the data packets ([0052]); transmitting data packets from a second subsystem to a first subsystem ([0054] lines 1-3); receiving the transmitted streaming data packets for processing in the first subsystem ([0057] lines 1-9, Fig. 7); sending respective ones of the security tag vectors from the first subsystem to the second subsystem ([0058]), responsive to the data packets and

the rules of processing ([0059] lines 1-3); and processing the received security tag vectors in the second subsystem to assure that the processing in the first subsystem is compliant with the defined rules of processing ([0052] lines 3-5, [0055], Fig. 7).

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. **Claims 2-5, 7-21, 23-30, 32-36, 38-51, 53, 57-64, 66-95, and 97-102** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Agrawal** in view of **Andrews (US 6,574,736)**, hereafter "Andrews".

3. Considering **Claims 10, 11, 38, 64, 77, 79, 80, 82-84, and 96-98** Agrawal discloses a first processing subsystem (a) for processing of streaming data packets ([0033] lines 1-3), responsive to defined rules for processing streaming data packets ([0038] lines 11-17), and (b) for generation and selectively sending of security tag vectors ([0052], [0058]); wherein the first processing subsystem is further comprised of a plurality of software logic modules each operable stand-

alone to provide a respective one of a plurality of subtask functions ([0033][0034], Fig. 1, Fig. 4).

Agrawal does not explicitly disclose a transformation controller for interlocking the plurality of software logic modules into a single logic program; wherein the combined functionality is only provided when the plurality of subtask functions are executed responsive to the single logic program. Agrawal does suggest the routing protocol that is used is Cluster Based Routing Protocol (CBRP), which is suitable for a large network of a number of nodes, each having an identifier (ID). The entire network 10 is divided into a number of overlapping or disjoint 2-hop diameter clusters as depicted in FIG. 1 ([0033][0034]).

Andrews discloses a transformation controller for interlocking the plurality of software logic modules into a single logic program (column 5- lines 63-65); wherein the combined functionality is only provided when the plurality of subtask functions are executed responsive to the single logic program (column 6- lines 18-33, col. 16- lines 16-31).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Agrawal by a transformation controller for interlocking the plurality of software logic modules into a single logic program; wherein the combined functionality is only provided

when the plurality of subtask functions are executed responsive to the single logic program as taught by Andrews in order to provide the advantages of object oriented programming. An advantage of object-oriented programming is the ability to incorporate logic for a particular set of related functions into a single software component. Consequently, software developers can build an application by assembling a set of software components, reusing proven software components without having to reexamine their logic. The ability to reuse software components (sometimes called "reusability") leads to more efficient application development. The two applications may be combined (or "composed") into an overall application, exchanging data among the software components (Andrews- col. 3- lines 18-37).

4. Considering **Claims 2, 3, 27, 28, and 42,** the combination of Agrawal and Andrews discloses a transmission/forwarding controller for stopping the sending of the streaming data packets responsive to the defined validation logic of the selectively transmitted security tag vectors (Agrawal- [0062] lines 11-19, Andrews- column 22- lines 1-9)).

5. Considering **Claim 4,** the combination of Agrawal and Andrews discloses the defined sequence of decryption keys are sent from the second subsystem to first subsystem responsive to the defined validation logic of the selectively transmitted security tag vectors (Agrawal- [0048] lines 1-6).

6. Considering **Claims 5 and 63,** the combination of Agrawal and Andrews discloses the processing of streaming data packets is further comprised of processing logic ([0033] lines 1-3); and wherein the processing logic is further comprised of at least one of: a privileges table, a privileges decision-tree, pseudo random rendering logic, a streaming data packet header processing privileges decision-tree, a security tag processing logic, a streaming data packet identification processing logic, a secure time-stamp processing logic, a processing of streaming data packets with secure time-stamps, watermarking information processing, fingerprinting information processing, stenographic information processing, data embedding information processing, digital signature information processing, and a processing of streaming data packets with secure time-stamps that is responsive to UTC (coordinated universal time) (Agrawal- [0052] lines 7-11, [0053] lines 5-8, Andrews- column 2- lines 66-67, column 3- lines 1-15)).

7. Considering **Claim 7,** the combination of Agrawal and Andrews discloses at least one of: the logic of the first processing subsystem, the defined rules for processing, and the security tag vector generation are further characterized as responsive to a at least one of: a predefined schedule, a secure time-stamp, renewable codes and parameters, updated codes and parameters, a predefined schedule received from the second subsystem, a secure time-stamp received

from the second subsystem, renewable codes and parameters received from the second subsystem, updated codes and parameters received from the second subsystem, a predefined schedule received from a third subsystem, a secure time-stamp received from a third subsystem, renewable codes and parameters received from a third subsystem, and updated codes and parameters received from a third subsystem (Agrawal- [0052] lines 7-11, [0053] lines 5-8, Andrews- column 1- lines 15-23, column 4- lines 42-46).

8. Considering **Claims 8, 9, and 81,** the combination of Agrawal and Andrews discloses at least one of: selected parts of the logic of the first processing subsystem, selected parts of the defined rules for processing, selected parts of the security tag vector generation, selected parts of the renewable codes and parameters, and selected parts of the updated codes and parameters are provided from an external storage medium which is at least one of: a smart card, a tamper-proof device, obfuscated storage, hidden storage, encrypted data storage, removable storage, a token card, and a metro card (Agrawal- [0041]- lines 19-25, Andrews- column 6- lines 64-67, column 7- lines 1- 14).

9. Considering **Claims 12, 14, 45, 46, 62, 72-74, 85, 99, and 100,** the combination of Agrawal and Andrews discloses an update/renewable controller providing at least one of: updated codes, updated parameters, update decryption codes, update decryption keys, update rendering codes, update playing codes, and

updated secure time stamp to the first subsystem (Agrawal- [0015], [0052] lines 7-11, [0053] lines 5-8, Andrews- column 1- lines 15-23, column 4- lines 42-46).

10. Considering **Claims 13 and 15,** the combination of Agrawal and Andrews discloses a security management server (SMS) for providing update/renewable information to the update/renewable controller (Andrews- column 2- lines 52-65).

11. Considering **Claims 16, 17, and 86-94**, the combination of Agrawal and Andrews discloses the first/second subsystem is further comprised of cryptographic/validation modules (Agrawal- Fig. 2- item 34, Fig. 8, Andrews- Fig. 17); and wherein the cryptographic modules provide for at least one of: program authentication, user authentication, cryptographic authentication, application authentication, encryption, a secure time-stamp, a digital signature, watermarking information, IPSec (IP Security) functionality, TLS (Transport Layer Security) functionality, and SSL (Secure Sockets Layer) functionality (Agrawal- Fig. 2- item 34, Fig. 8, [0051]-[0052], Andrews- Fig. 17, col. 17- lines 10-13).

12. Considering **Claims 18-21, 53, and 68-71,** the combination of Agrawal and Andrews discloses the first subsystem further is included within a media player (Andrews- Fig. 1- item 30 and item 48), the media player is directly attached to at least one of: a video display, a TV display, a computer monitor, a handheld display, an audio speaker, a stereo audio system, a digital output system, an

analog output system, and a media play buffer (Agrawal- [0041] lines 19-25, Andrews- column 6- lines 64-67, column 7- lines 1-14, Fig.1 – item 47), the media player performs at least one of: deleting streaming data packets after processing, deleting streaming data packets within a predefined time interval after processing, deleting streaming data packets after a defined number of times of processing, preventing copying of the streaming data packets, preventing printing of the streaming data packets, preventing sending of the streaming data packets, encrypting video rendering of content received in the streaming data packets, pseudo random video rendering of content received in the streaming data packets, encrypting video rendering of content stored in the first subsystem, and pseudo random video rendering of content stored in the first subsystem (Agrawal- [0051]-[0052], Andrews- column 2- lines 52-65, Fig. 15).

13. Considering **Claims 23, 24,** and **26,** the combination of Agrawal and Andrews discloses the second subsystem further includes a media server whose operations are responsive to the security tag vectors sent from the first subsystem (Andrews- column 2- lines 52-65).

14. Considering **Claims 25 and 30,** the combination of Agrawal and Andrews discloses there is a plurality of the first subsystems, each coupled to the network and receiving streaming data packets from the second subsystem and a plurality of second subsystems coupled to the network, each sending a respective

plurality of streaming data packets to the first subsystem (Agrawal- [0034]-[0035], Andrews- column 6- lines 27-40).

15. Considering **Claim 29,** the combination of Agrawal and Andrews discloses the streaming data packets are sent using at least one of: Multicast, IP (Internet Protocol) Multicast, Secure IP Multicast, Group Key Management Architecture, Multi-Party Non-Repudiation Protocol, Group Communications, and Secure Group Communications (Agrawal- [0034]-[0035], Andrews- column 10- lines 60-67, column 11- lines 1-15).

16. Considering **Claims 32, 51, and 102,** the combination of Agrawal and Andrews discloses the first subsystem is at least one of: a wireless device, a handheld device, a Wi-Fi device, a device operating in accordance with IEEE 802.11 family of standards, a device operating in accordance with IEEE 802.15, a 2.5G cellular telephone, a 3G cellular telephone, a 4G cellular telephone, a 5G cellular telephone, a personal computer, a set-top box, a device operating in accordance with UMTS (Universal Mobile Telephone System), and a device operating in accordance to the IEEE 802.3 family of standards (Agrawal- [0004], Andrews- column 6- lines 27-33).

17. Considering **Claims 33-36, and 44,** the combination of Agrawal and Andrews discloses the first subsystem further comprises logic for generating and sending

encryption keys to the second subsystem; and wherein the second subsystem uses the encryption keys for encrypting the streaming data packets prior to sending them., the encryption key is provided at least one of: periodically, at random times, at predefined time intervals, responsive to validating the received security tag vectors, and at predefined times derived from coordinated universal time (UTC) (Agrawal- [0051]-[0053]).

18. Considering **Claims 39-41, 66, 67, 75, 76, 78, and 101,** the combination of Agrawal and Andrews discloses producing the pseudo-random sequence of security tag vectors utilizing computation by at least one of: applying a pseudo-random generator, applying a pseudo-random function, applying a cryptographic function, applying an encryption function, applying a scrambling subroutine, applying an authentication function, applying a digital signing function, applying a cryptographic hash function, applying a subroutine, applying a computational logic module, applying a symmetric cryptography function, applying an asymmetric cryptography function, employing a cryptographic key, employing a cryptographic seed, employing an encrypted software, employing an obfuscated software, employing a hidden program, employing watermarking information, employing fingerprinting information, employing digital signature information, employing logic with a set of parameters, employing a hardware module, employing a smart card, employing a portable device, and employing a distributed protocol (Agrawal- [0052], [0059]).

19. Considering **Claim 43,** the combination of Agrawal and Andrews discloses a smart card that is part of the first computing element, and wherein selected modules and parameters of the plurality of software logic modules and parameters reside on the smart card (Agrawal- [0041] lines 19-25, Andrews- column 7- lines 8-14).

20. Considering **Claim 47,** the combination of Agrawal and Andrews discloses the renewing is performed in at least one of: periodically, at random times, at predefined times, at predefined times derived from coordinated universal time (UTC), responsive to receiving data by the first computing element, responsive to sending the security tag vectors, and responsive to sending data by the second computing element (Agrawal- [0012], Andrews- column 4- lines 42-46).

21. Considering **Claim 48, 49, and 50,** the combination of Agrawal and Andrews discloses erasing data from one of: solid state, a magnetic storage device, and an optical storage device, is performed responsive to at least one of: after predefined time, after the data was output to an output device, and after the data was output predefined number of times to an output device (Agrawal- [0012], Andrews- column 12- lines 53-67).

22. Considering **Claims 57-61,** the combination of Agrawal and Andrews discloses the tag generator includes a sequence number as part of the security tag vector and generates a comparison sequence number for selective comparison to the sequence number, the tag generator provides a secure time-stamp for selective comparison to the secure time-stamp that is part of the security tag vector (Agrawal- [0052]-[0054], [0059], Fig. 8- item 152).

23. **Claims 6 and 22** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Agrawal** and **Andrews** in view of **Capitant (US 2003/0078891)**, hereafter "Capitant".

24. Considering **Claims 6 and 22,** the combination of Agrawal and Andrews discloses the processing of streaming data packet is constructed with codes and parameters in accordance with trusted computing specifications, trusted computing based principles, validation of watermarking information, IPSec (IP Security) functionality, TLS (Transport Layer Security) functionality, and SSL (Secure Sockets Layer) functionality (Agrawal- [0061] lines 7-12).

The combination of Agrawal and Andrews does not explicitly disclose the processing of streaming data packet is constructed with codes and parameters in accordance with XrML (Extensible Rights Markup Language).

Capitant discloses the processing of streaming data packet is constructed with codes and parameters in accordance with XrML (Extensible Rights Markup Language) ([0045]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Agrawal and Andrews by using XrML as taught by Capitant in order to provide a universal method for specifying rights and issuing conditions (licenses) associated with the use and protection of content (Capitant- [0045] lines 5-7).

25. **Claim 65** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Agrawal**

and **Andrews** in view of **Drake (US 6,006,328)**, hereafter "Drake".

26. Considering **Claim 65,** the combination of Agrawal and Andrews does not explicitly

disclose the single logic program is written to be immune to reverse generation.

Drake discloses the single logic program is written to be immune to reverse generation (column 3- lines 45-49).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Agrawal and Andrews by the single logic program is written to be immune to reverse generation as taught by Drake provide computer software having enhanced security features, to a process which substantially enhances the security of computer software (Drake- column 3- lines 32-37).

Conclusion

1. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- US 6,990,528 – End to end context via reliable datagram.
- US 6,182,146 – Identification of protocols.
- US 6,418,478 – High-speed data transfer.
- US 2003/0078890 – XrML representation of the context package.

2. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Randal D. Moran whose telephone number is 571-270-1255. The examiner can normally be reached on M-F: 7:00 - 4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Randal D. Moran
/RDM/

5/31/07

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100